Measuring Risk

"Helping computer system owners conquer the risk of the cyber-frontier"

This presentation is: UNCLASSIFIED

Cyber Defense Agency, LLC

jwallner@CyberDefenseAgency.com
301-928-7547

sevans@CyberDefenseAgency.com
410-215-5709

Introduction

- Estimating risks of cyber attacks to complex systems with accuracy and confidence is difficult
- CDA has developed REVEAL, a risk assessment process with supporting tools
- REVEAL has been used for 7 years to successfully solve difficult and contentious problems for the DoD
- REVEAL is complimentary to current control systems risk assessment tool prototypes

The Risk Equation Challenge

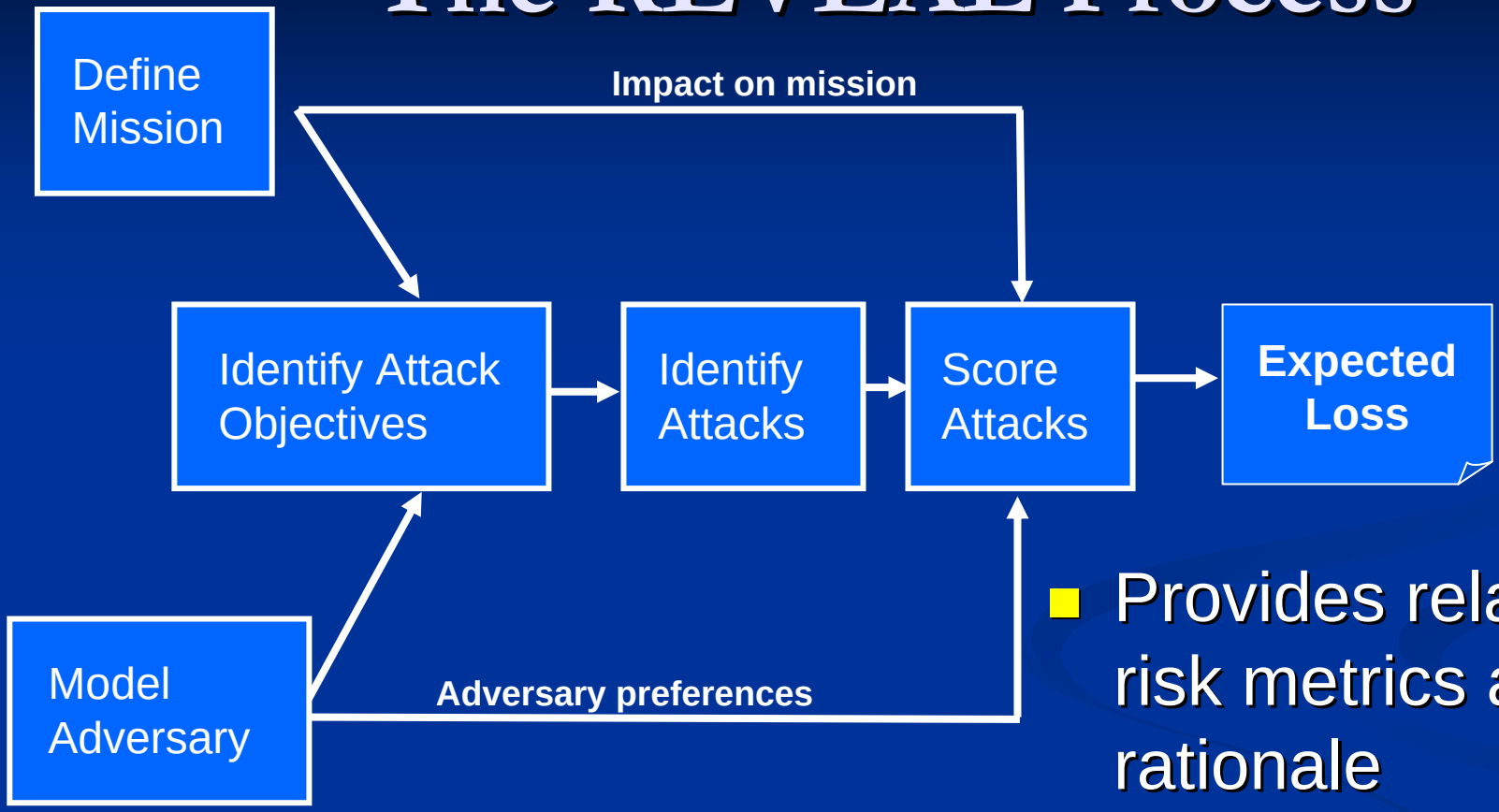
- The Classical Risk Equation: $R_e = P_e * C_e$
  - Challenge: Estimating risk with confidence
  - Approach: Decompose the risk equation into quantifiable atomic units and model the adversary
    - Related Work: McQueen, Boyer, Flynn and Bietel:

      $P_e = P_t * P_a * P_b * P_s * P_c$

      $Threat_i = f(Intent_i, Capability_i, Opportunity_i)$

      Estimates % Risk Reduction

The REVEAL Process



- Provides relative risk metrics and rationale
- Focuses on attacker and mission
- Builds on existing attack and adversary database, so is efficient and reusable

Adversary Reference Manual

List of Adversaries

- Government / Nation State at Peace
- Military / Nation State at War
- Economic Competitor
- Terrorists
- Organized crime
- Hackers
- Crackers
- Insiders
  - Malicious
    - Co-opted
    - Non-co-opted
  - Non-malicious
    - Human error
    - Social engineering
- …

For each adversary

Text description of typical behavior

Attack Capabilities List

- HUMINT
- SIGINT
- CNA
- SpecOps
- EW
- Lifecycle
- M&C
- Social Engineering
- Insider access
- Kinetic Weapons

For each adversary / attack capability pair

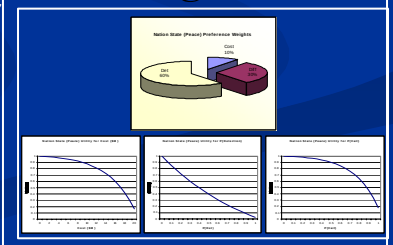
Adversary skill level (none to VH)

Adversary Characteristics

- Monetary Resources
- Difficulty
- Detectability

For each adversary characteristic

- Utility Curves
- Preference Weights



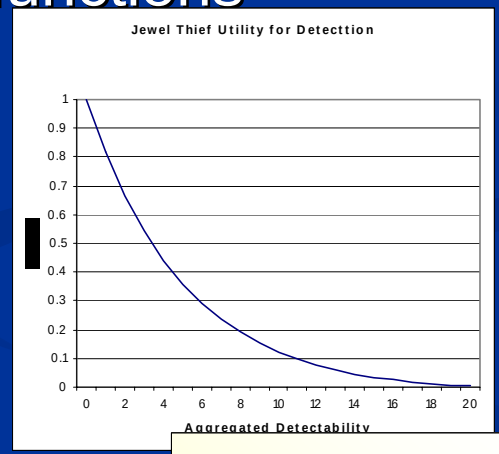
Attack Objectives and Motivations

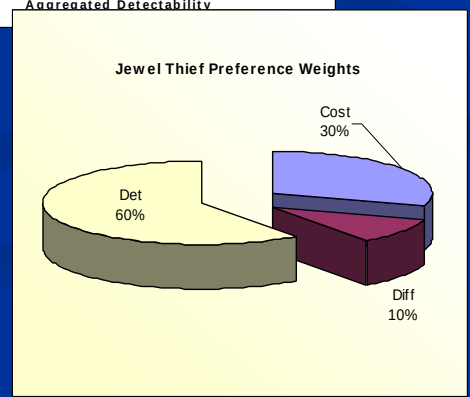
Attack Scores

Attack #1	Cost	Difficulty	Detection
Break in Control facility	$1,000	9	8
Gain access to control system	$0	5	2

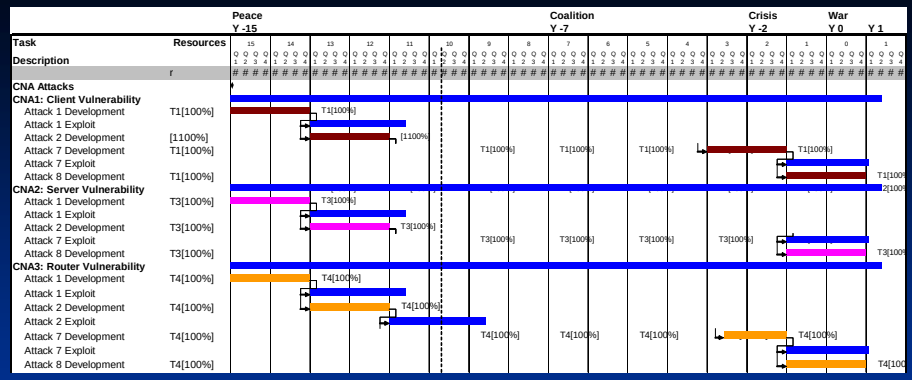
Aggregated Scores	$1,000	14	10
Adversary Utility	1.0	0.20	0.12
Adversary Weights	0.30	0.10	0.60
Product	0.30	0.02	0.07
		Weighted Sum:	0.39

- Once the attack steps have been scored, the aggregated system attack scores are converted to utilities using the adversary preference functions





Attack Strategy



- Each adversary has constrained resources (time, money, manpower, risk tolerance) – so they cannot afford to exploit every available attack
- The adversary must develop an attack strategy that maximizes the return on their attack investments
- The overall attack strategy represents the risk exposure to the defender from which the expected loss due to cyber attacks can be calculated

Attack Strategy transforms numeric results into a realistic attack campaign to help the defender better understand the adversary

Conclusions and Frontiers

- REVEAL provides relative risk metrics based on adversary models, attack scores and utility theory
  - CDA is currently researching replacing the relative risk metric with an absolute risk metric
- REVEAL is supported with an adversary library, attack knowledge base and suite of automated tools
  - CDA would like to extend REVEAL with additional adversaries and attacks specific to control systems
  - CDA is working on a more sophisticated knowledge base and additional automated tools